TOP SECRET "U"

TICOM/I-16

NOTES ON INTERROGATION OF AMTSRAT SCHWABE AND OBFKMSTR. WARZECHA ON RUSSIAN NAVAL CYPHERS

The interrogations on which these notes are based were carried out by Captain ROYFFE I.C. on 18th, 20th and 21st. June, 1945, at the Signals School, FLENSBURG.

Details of the individuals, both of whom belonged to OKM, 4 SKL III, are as follows;-

SCHWABE, Wilhelm, Amtsrat, Head of Section III FC.

WARZECHA, Alfons, Obfkmstr. (B), official number No. 1797/37S member of Section IIIr.

TICOM
26 June, 1945

Copy No. 16
No. of pages 4-

DISTRIBUTION

British
1. Director
2. D.D.3
3. D.D.4
4. D.D. (N.S.)
5. D.D. (M.W.)
6. D.D. (A.S.)
7-8. A.D. (C.C.R) (2)
9. Col. Leatham

U.S
25-26. OP 20-G (2)
(via Lt. Pendergrass)
27. G-2 (via Lt. Col. Hilles)
28-29. S.S.A. (2)
(via Major Seaman)
30. Director, S.I.D. ETOUSA
(via Lt. Col. Johnson)

Ticom
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt. Col. Johnson
17. Major Seaman
18. Lt. Eachus
19. Lt. Vance
20. Capt. Cowan
21. Lt. Fehl
22-24. Ticom Files (3)

Additional
31. Capt. Royffe

I16

NOTES ON INTERROGATION OF

AMTSRAT SCHWABE AND WARZECHA

18, 20 & 21 June 1945

Russian Naval Ciphers

Systems were divided into Baltic, North Sea and Black Sea. Similar systems were used in all three areas, and will therefore be treated as a whole. There was a further subdivision into main and subsidiary systems. Main systems were used by shore stations and large units, and were 4 & 5-figure. Subsidiary systems were used by small ships, etc., and were 2, 3 and 4-figure. The 5-fig. were usually subtractor (including one-time pads), the 4-fig. partly subtractor and partly substitution, the 2 and 3-fig. were substitution tables. Besides purely Naval systems, there were Fleet Air Arm systems.

The main Baltic system before the war was 5-fig. subtractor, with an underlying 5-fig. limited book. The subtractor was 300 groups, and changed daily. At the beginning of the war this was replaced by a 4-fig. subtractor system, the subtractor being derived by simple substitution (3 different letters = 1 figure) on the clear text of a book called the "History of the Communist Party". Indicators formed by adding text groups together (e.g. 3rd & 5th message groups) showed page and line for starting the subtractor. This was in turn replaced by another 4-fig. subtractor system, which contained a lot of Fleet Air Arm traffic. This was only partly solved. Then there was a 5-fig. double subtractor (not solved). Lastly, several 5-fig. systems, one of which was 4-fig. disguised as 5-fig. The subtractor was 5-fig., and the 5th subtractor figure of each group was put in as a filler. These clear subtractor figures were indexed to build up depths, but there was not enough material to lead to a complete solution.

Besides the above there was a subsidiary small-ship system, consisting of a 4-fig. code with only about 22 pages, groups being enciphered on a bigram substitution table for the page, and single-fig. substitution tables for each margin figure. These tables changed twice daily, at 0600 and 1800 hrs. At the end of July 1944 this was varied, the new system being also a bigram substitution table for the page, and up to 6th Sept. 1944 a single column substitution for both 3rd and 4th figures; after 7th Sept. 1944 there was again one substitution column for the first margin figure, and another one for the second. This system was called "GRAUDENZ" by the Germans, and was the most important system for them (i.e. gave best results) up to the end of the war. The substitution tables were as follows:-

	0	1	2	3	4	5	6	7	8	9	
											(b)
0	22	23	24	25	01	02	03	04	11	12	4
1	13	14	15	89	90	91	92	53	54	55	1
2											0
3											6
4											5
5					&c.						2
6											7
7											3
8											9
9											8
(a)	4	6	5	1	0	7	2	9	8	3	

The bigram in the large square was the page, e.g. 10 = 13, 08 = 11, &c. The code book was still limited to 22 or 23 pages, but each page had several designations, always consecutive numbers, thus the first page in the book could be 15, 16, 17, 18. The decipher squares built up by the

I16

Germans could therefore be simplified, e.g.

0 1 2 3 4 5

0 12 12 12 12 26 26 instead of 12 13 14 15 26 27 etc.

The third figure (first margin) was simple substitution on the single row (a) underneath the square, and the 4th figure (second margin) simple substitution on the column (b) to the right of the square. (e.g. margin 05 = 42, 06 = 47, &c.)

These substitution tables changed very often, sometimes even from message to message, but one table could be used quite a number of times. Depths could therefore be built up and read, as the underlying book was partly known.

The indicator system was not solved. They intended to read a large number of messages, and then see how the indicators worked; but the end of the war intervened before they could carry out this plan. They did see, by reading messages, that the indicator was in the 5th and 6th text groups, because the clear text read straight across from the 4th to the 7th. This was as far as they got.

Asked whether there was an unreciphered 4-fig. system, they said they had never heard of one.

Three-fig. systems were very simple, consisting of a small code reciphered on a 3-column simple substitution table, cols. 1-2-3 enciphering the corresponding code groups. This substitution changed daily. In the North Sea, a large number of recognition signals were sent on this system, and were sent two days in advance, which was very helpful for German aircraft; this also applied to Black Sea traffic. The German planes, on approaching a Russian airfield, would give the correct signal, and the field would be lighted up.

This system was also used to give positions of ships, and the 2-fig. times, degrees and so on would be turned into 3-fig. by prefixing a 0, e.g.

18 hrs. 24 mins. 12° 22' E 68° 15' N

= 018 024 012 022 068 015 (these groups were then substituted by the table).

Five-fig. Baltic & North Sea: Several systems were in force, of which the main ones were in effect one-time pads. The key was thought to be a subtractor book, with 100 groups per page, each page containing an indicator; messages started at the top of the page, and if shorter than 100 groups, the rest of the page was not used. (No message exceeded 103 groups, including 3 indicator groups). Sending stations were each allotted a number of indicators, which were struck off as used. It happened, however, in July, August and September '44, that Chabarovo was not given enough indicators, and used each from 2 to 10 times, thus providing plenty of depths (in October this was rectified). These depths showed the traffic to be 4-figure, with the 5th subtractor figure put in as a filler. There was not enough of this to enable the book to be more than partially solved, and there was no sign of depths after September '44 from any station.

A specimen indicator system is as follows (there were many different ones, but all worked more or less in the same way):

Penult. group of message: 2 4 3 7 8

I16

The 4th fig. was a check on the last, the final bigram being limited to the series 01, 12, 23 &c. The first fig. was added to the second: 2 plus 4 = 6; mark the 6th group from the start of the message. Then add the third to the fifth: 3 plus 8 = 1; mark the first group counting back from the penult. The indicator is given by subtraction of these groups one from the other.

Five-figure books early in the war were limited. One book had page trigrams, all odd or all even. Another had groups built up on a formula, e.g. $\frac{a+b}{2} + c - d + e = x$

If x = 0, the group was the name of a ship or unit; if x = 5, it would be a numeral, time, date, &c.

The all-odd or all-even page limitation was useful for building up depths. First trigrams of message groups were indexed for parity. This, however, could not be carried far enough to break the system, owing to lack of material. These limitations were not apparent in later books.

A further 5-fig. system was a development of the 3-fig., the first bigram representing the second code figure, the last bigram the third code figure, and the middle single figure the first code figure, which was limited. This system was by substitution tables. This was a Met. system.

One 3-fig. system had a daily change of the first bigram, but the last figure remained constant (German name "Vardö" - North Sea traffic). This was a single code sheet, with only 100 groups (10 bigrams, each followed by 0-9). No further recipherment.

There was a 6-fig. Met system in use, with underlying international weather code.

In the Black Sea there were two 4-fig. subtractor systems, one with an alphabetic book and one with a hatted book. These originally used the same subtractor. Keys changed every 3 to 5 days. The indicators were variable position subtraction, and sometimes the figures had to be transposed before subtraction. This was replaced by a 5-fig. system, which was only observed, not worked on, as North Sea and Baltic traffic was by then more important.

Asked about collaboration with the Finns, they said it was rather a matter of competition, although results were exchanged. The Finns were very good, and had excellent opportunities for picking up Baltic traffic. The Finns once solved a 5-figure double-subtractor for one day.

Asked whether one-time pad systems were used on complicated net-works, they said no.

Regarding indicators of 5-figure systems, besides the actual indicator there were groups giving length check, sender's signature trigram, etc., and sometimes the priority was indicated by the middle figure of the last group.

Word Codes, machines and Agents' systems were all equally unknown.

- - - - - - - - - -

WARZECHA complained that they had been given insufficient time to refresh their memories on details of these different systems; he was asked to write at leisure a more detailed report, and pass it on through TRANOW to our people. This he promised to do.

The 4th fig. was a check on the last, the final bigram being limited to the series 01, 12, 23 &c. The first fig. was added to the second: 2 plus 4 = 6; mark the 6th group from the start of the message. Then add the third to the fifth: 3 plus 8 = 1; mark the first group counting back from the penult. The indicator is given by subtraction of these groups one from the other.

Five-figure books early in the war were limited. One book had page trigrams, all odd or all even. Another had groups built up on a formula, e.g. $\frac{a+b}{2} + c - d + e = x$

If x = 0, the group was the name of a ship or unit; if x = 5, it would be a numeral, time, date, &c.

The all-odd or all-even page limitation was useful for building up depths. First trigrams of message groups were indexed for parity. This, however, could not be carried far enough to break the system, owing to lack of material. These limitations were not apparent in later books.

A further 5-fig. system was a development of the 3-fig., the first bigram representing the second code figure, the last bigram the third code figure, and the middle single figure the first code figure, which was limited. This system was by substitution tables. This was a Met. system.

One 3-fig. system had a daily change of the first bigram, but the last figure remained constant (German name "Vardö" - North Sea traffic). This was a single code sheet, with only 100 groups (10 bigrams, each followed by 0-9). No further recipherment.

There was a 6-fig. Met system in use, with underlying international weather code.

In the Black Sea there were two 4-fig. subtractor systems, one with an alphabetic book and one with a hatted book. These originally used the same subtractor. Keys changed every 3 to 5 days. The indicators were variable position subtraction, and sometimes the figures had to be transposed before subtraction. This was replaced by a 5-fig. system, which was only observed, not worked on, as North Sea and Baltic traffic was by then more important.

Asked about collaboration with the Finns, they said it was rather a matter of competition, although results were exchanged. The Finns were very good, and had excellent opportunities for picking up Baltic traffic. The Finns once solved a 5-figure double-subtractor for one day.

Asked whether one-time pad systems were used on complicated net-works, they said no.

Regarding indicators of 5-figure systems, besides the actual indicator there were groups giving length check, sender's signature trigram, etc., and sometimes the priority was indicated by the middle figure of the last group.

Word Codes, machines and Agents' systems were all equally unknown.

- - - - - - - - - -

WARZECHA complained that they had been given insufficient time to refresh their memories on details of these different systems; he was asked to write at leisure a more detailed report, and pass it on through TRANOW to our people. This he promised to do.